Retraction

Retracted: Application Research of Data Encryption Algorithm in Computer Security Management

Wireless Communications and Mobile Computing
Received 18 July 2023; Accepted 18 July 2023; Published 19 July 2023

Copyright © 2023 Wireless Communications and Mobile Computing. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

1. Discrepancies in scope
2. Discrepancies in the description of the research reported
3. Discrepancies between the availability of data and the research described
4. Inappropriate citations
5. Incoherent, meaningless and/or irrelevant content included in the article
6. Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article’s content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

Research Article

Application Research of Data Encryption Algorithm in Computer Security Management

Qianru Gong

Electronic Information Engineering College, Henan Polytechnic Institute, Nanyang, Henan 473009, China

Correspondence should be addressed to Qianru Gong; 31115328@njau.edu.cn

Received 4 June 2022; Revised 22 June 2022; Accepted 1 July 2022; Published 14 July 2022

Academic Editor: Balakrishnan Nagaraj

Copyright © 2022 Qianru Gong. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In order to promote the research process of information security in the whole society, improve the safety factor of computer data communication, strengthen computer security management, the author proposes a computer data encryption strategy that combines the strong security of the 3DES encryption algorithm and the asymmetric encryption advantages of the RSA algorithm. Through the detailed analysis of DES encryption algorithm and 3DES encryption, creatively uses the RSA encryption algorithm to improve the single 3DES algorithm, consolidates the performance of the 3DES encryption algorithm to ensure data communication, and ensures the data integrity, better improve encryption performance. Experiments show that: The proposed encryption algorithm improves security performance by 10 times, and the response efficiency is only 1 ms away from other algorithms, compared with other algorithms, it has better encryption performance and is suitable for actual computer data communication scenarios. Conclusion: The encryption algorithm proposed by the author has achieved good results in terms of security performance and response efficiency, it is suitable for actual computer data security communication and can effectively improve computer security management.

1. Introduction

With the wide application of network technology, the establishment and development of personal communication, e-mail, electronic payment, automatic retail business, etc., various computing and communication systems have become an important part of the human living environment, they collect, analyze, store, display and disseminate information in multimedia formats, and as independent products or combined with other physical products to become human political, economic, military and cultural services. People should be concerned about their own information security issues [1]. Most of modern social work data is transmitted at high speed by computer as a carrier, whether it is personal or corporate data, there is a danger of being hacked and deciphered, resulting in different degrees of loss, as shown in Figure 1. In this context, how to use all kinds of information safely and effectively has become an important cornerstone to ensure the development of human society; How to ensure that information is not illegally stolen, eavesdropped, forged and tampered with during the transmission and processing of information on the public network, that is, the issue of information authentication and confidentiality, has become a problem that people are concerned about, therefore, the theory of encryption algorithm and its implementation technology have become an important research field in modern information science and technology, and have been paid more and more attention [2]. On the other hand, with the continuous improvement of the level of social informatization, especially the rapid development of Internet technology, there are more and more network applications, how to protect the confidential data in the application, it can also effectively prevent external attacks, which is a major problem faced by network applications [3]. Therefore, in order to promote the research process of information security in the whole society, improve the security factor of computer data communication, and strengthen computer security management, the article deeply explores the computer security technology, creatively constructs a hybrid encryption strategy, uses the triple DES algorithm to improve the data encryption security factor, and uses the RSA algorithm to encrypt the triple DES algorithm key to achieve double
encryption guarantee, so as to realize the computer Communication security [4].

2. Literature Review

For computer security data encryption algorithm, Zhao, C. et al. proposed a general AES encryption algorithm, choosing a data encryption scheme with fixed key length and fixed data block length [5]. This can ensure the security of data encryption while ensuring the speed of encryption and decryption, and at the same time, it can also reduce the complexity of program design, and thus reduce the development workload. Lin, C. et al. proposed a secure hash algorithm MD5, inputting two different plaintexts will not get the same output value, and the original plaintext cannot be obtained according to the output value, that is, the process is irreversible [2]. Cai, W. et al. proposed an IDEA algorithm, which belongs to the class of block encryption algorithms in cryptography. IDEA uses a key with a length of 128 bits and a data block size of 64 bits. In theory, IDEA is a “strong” encryption algorithm, and there is no effective attack scheme for this algorithm [6]. Ebinazer, S. E. et al. proposed a Blowfish encryption algorithm, the core of the algorithm lies in the sub-key generation, which expands the variable-length key into a sub-key array with a total length of 4168 Bytes. A large number of subkeys are used in the algorithm, and the subkeys depend on the user key, the updated subkey array is used in the actual encryption and decryption process. Another feature of it is that two parts of the file are encrypted at the same time in each round, which increases the strength of the cipher [7]. Liu, Xin, etc. proposed algorithms such as square and Shark, the biggest advantage of these algorithms is that they can theoretically prove that the algorithm is secure for differential cryptanalysis and linear cryptanalysis. And with the collection of the AES algorithm, the research on its block cipher has entered a new research stage, the 15 candidate algorithms of AES reflect the current level of block cipher [8]. Liu, Q. et al. proposed the AES encryption algorithm, which is an advanced encryption standard in cryptography, the encryption algorithm adopts a symmetric block cipher system, the minimum supported key length is 128 bits, 192 bits, and 256 bits, for 128 bits, the algorithm should be easy to implement in various hardware and software [9]. Alenezi, M. et al. proposed a selective data encryption algorithm (SDEA). The principle of the algorithm is to use different privacy classification methods to selectively encrypt data under the unit time limit, the purpose is to achieve the minimum execution time required by the practical application, use selective data encryption algorithms to maximize the protection of big data privacy [10]. Based on the current research, the author addresses the need for data encryption for data managed by computer security, a strong security combined with 3DES encryption algorithm is proposed, computer data encryption strategy based on the advantages of RSA algorithm asymmetric encryption, through the detailed analysis of DES encryption algorithm and 3DES encryption, creatively use the RSA encryption algorithm to improve the single 3DES algorithm, and the superiority of the performance of the encryption algorithm is confirmed by experiments.

3. Research Methods

3.1. Encryption Theory and Experiments Have Confirmed the Superiority of the Encryption Algorithm Performance. Symmetric encryption is also known as private key encryption algorithm, high-efficiency encryption and fast encryption are its main features. The encryption and decryption processes use the same key in the symmetric encryption algorithm, so the security of the symmetric encryption algorithm is directly related to the confidentiality of the key. If symmetric encryption is used in the process of ensuring data security, both parties should agree on the key before transmitting data, and at the same time, the determined key should be properly stored [11]. If one of the parties leaks the key, the entire communication process will be cracked, data...
Encryption Standard (DES) is a typical system of symmetric encryption. When doing asymmetric encryption algorithms, there should be keys for two different processes, encryption and decryption. The public key (referred to as "public key") is used for encryption, and the private key (referred to as "private key") is used for decryption. In order to decrypt data encrypted by the public key, the corresponding private key must be used; At the same time, the corresponding public key must be used to decrypt the data encrypted by the private key [12]. The public key can be published and sent to other requesting users. However, the private key must not be leaked, and should only be kept by Party B. During data transmission, the transmission security problem of the key in the symmetric encryption algorithm can be well solved. However, when the asymmetric encryption algorithm is performed, it takes a lot of time to encrypt and decrypt, compared with the symmetric encryption algorithm, the speed is far from enough, and it is more suitable for the encryption of a small amount of data.

3.2. Security Analysis of Computer Data Communication Based on DES Algorithm. The DES data encryption algorithm is an encryption standard in many foreign countries, at the same time, it gives a high degree of affirmation to this algorithm, and believes that this encryption algorithm is more consistent with its own data encryption requirements: First, the data protection function of the DES data encryption algorithm is relatively strong, and at the same time, it can effectively prevent the illegal leakage of data, and can timely prevent the occurrence of malicious modification of undetected related data; Second, the DES data encryption algorithm is extremely complex and difficult to decipher. At present, the exhaustive method is the only way to decipher the encryption algorithm in the world, in other words, if someone wants to decipher the DES data encryption algorithm, they must spend a lot of time and energy, and compared with the related benefits they get, it is ultimately a multiplier effect. Even if the modern computer chosen can perform millions of calculations per second, it will take about 2000 years to find out the deciphering method using the exhaustive method; Third, although the DES data encryption algorithm is relatively complex, its overall cryptographic system does not need to have overly complex characteristics, for the encryption key system, the DES encryption algorithm is the basic and core part; Fourth, in the process of summarizing the DES data encryption algorithm, it can be found that the secondary encryption method is extremely effective, it is widely used in data encryption in the communication and financial industries, and the ATMs that we encounter in our daily lives use this data encryption algorithm [13]. Based on the DES data encryption algorithm to ensure the communication security between computers, it is to encrypt the plaintext data generated by the computer communication with the secret key to obtain the communication ciphertext, and then transmit the ciphertext to the receiving end to decrypt the recovered plaintext based on the key, this is the basic principle of computer secure communication. The DES algorithm divides data into multiple groups, and uses this block-encrypted symmetric encryption algorithm on both the input and output ends, but the key settings are different; The 64-bit plaintext is input from the input end of the encryption algorithm, and the 64-bit ciphertext is output from the output end; The DES key has a length of 56 bits, which has the flexibility to be modified at any time [14]. In essence, the DES data encryption algorithm is highly scientific and open to the outside world. Therefore, in terms of computer communication technology, it is relatively simple to analyze and improve the DES data encryption algorithm. The main methods are as follows: When actually optimizing the computer communication technology, the corresponding technology type can be used in combination with the DES data encryption algorithm, and the computer mode and analysis strategy can be appropriately selected. After the technicians have a detailed understanding of the calculation method and working principle of the DES data encryption algorithm, with the help of the data encoding and powerful programming language of the computer system, effectively analyze and improve the entire DES data encryption algorithm system, compare the different applications of each algorithm for different encryption objects and computing environments, at the same time, the computer can also use the hard disk data to calculate the application program in the DES data encryption algorithm, so as to avoid leaking file information due to incorrect data. At the same time, the program of the same type should also be set in the computer encryption card, and a backup should be made [15]. During the establishment of the data encryption module, because the computing speed of computer communication technology and computer software is very fast, and at the same time, the calculation process is also very meticulous, so in the process of designing and perfecting the DES data encryption program, the expansion problem of the algorithm should be considered. Therefore, the principle of DES data encryption algorithm practice is summarized as follows: DES data encryption algorithm uses 56-bit security key to encrypt 64 data in real time, and generates key encryption after 16 rounds of encoding activities; During each round of encoding work, the S box stores 64 data and keys; Data replacement work is performed at the beginning and end of 16 rounds of encoding and between two rounds of encoding, the key is based on a special replacement rule to obtain a 48-bit key, and the data sequence is mixed; Based on the above encryption operation, the original communication data position is reconstructed, which can be safely output, after the receiving end receives the data, the decryption operation is performed to restore the original state of the communication data, thereby realizing the safe communication transmission of computer data.

3.3. Encryption of Computer Data Plaintext Based on 3DES. With the enhancement of the software and hardware capabilities of computer operations, the general DES encryption algorithm is easy to be cracked. In order to improve the security of computer data communication, the key length of the DES encryption algorithm is extended, and the attack on the encryption method by the brute force method is reduced, and the 3DES algorithm with improved form and improved security performance is obtained, it is equivalent
to applying the DES encryption algorithm three times to each data block, expanding the encryption application range of the original DES algorithm [16]. The 3DES data encryption algorithm sets three keys to encrypt the computer communication data, the defined keys are ka, kb, and kc, respectively, thereby extending the key to a length of 168 bits, Figure 2 shows the principle of the 3DES algorithm based on three key encryption.

The data plaintext and ciphertext in the communication process are defined as W and M, respectively, and the plaintext is encrypted by ka, kb and kc. The encryption process of the 3DES algorithm is described as \( W = E_{kc}[D_{kb}[E_{ka}[M]]] \), and the decryption process is described as \( M = D_{ka}[E_{kb}[D_{kc}[W]]] \). Considering that the length of the 3DES key is extended and the encryption efficiency is weakened, in order to prevent the encryption speed from being too low, \( kc = ka + kb \), the corresponding key length is 112 bits, which can guarantee the security requirements of most computer communications.

3.4. 3RSA Encryption Algorithm. In order to consolidate the 3DES encryption algorithm to ensure the performance of data communication, the RSA encryption algorithm is used to improve the single 3DES algorithm, and the 3DES algorithm key is encrypted, in this way, the security can be enhanced on the basis of ensuring the operation efficiency of the algorithm encryption, and provide a double guarantee for the security of computer communication; This method is a new hybrid data communication encryption technology formed by drawing on the advantages of 3DES algorithm and RSA encryption algorithm. The RSA encryption algorithm belongs to the asymmetric encryption algorithm, which uses both public key and private key [17]. The RSA algorithm has good security for encrypted communication data, and the algorithm is easy to implement, it can be said that RSA is the most widely used among many asymmetric encryption algorithms. Before the server receives the communication data, the RSA algorithm is used to perform encryption processing to generate the key. In the process of generating the private key based on RSA, the message needs to be mapped into an integer, that is, a block cipher, and the data owner knows the private key algorithm. In the process of RSA decryption, the key function is to verify, the data integrity is guaranteed, and the security of computer users is greatly improved. Key generation, plaintext encryption, and ciphertext decryption are the main steps of the RSA algorithm, and a key needs to be generated before encryption. The steps of RSA algorithm key generation are as follows:

Step1: Choose two arbitrary prime numbers \( c \) and \( v \) to determine the input for key generation.

Step2: Find the product \( i = c \times v \) of two prime numbers, then \( \phi(i) = (c - 1) \times (v - 1) \).

Step3: Select an integer \( e \) above \( c \) and \( v \) as the encryption key under random conditions, and let the greatest common divisor \( \gcd(e, \phi(i)) = 1 \).

Step4: Define \( y \) as the decryption key of the algorithm, and \( ye = \text{mod}\phi(i) = 1 \), further deduce \( ye = k\phi(i) + 1 \), and the value of \( k \) is an integer not less than 1; If you want to get the key \( y \), you need to know \( e \) and \( \phi(i) \).

Step5: Among the parameters of the above process, \( i \) and \( e \) are values that can be disclosed, and \( y \) is a value that needs to be stored secretly. The encryption and decryption methods of the RSA algorithm are shown in formula (1) and formula (2):

\[
W = E(M) = M^{e \mod i} \tag{1}
\]

\[
W = D(W) = M^{e \mod i} \tag{2}
\]
In the above formula, the plaintext and ciphertext are \( W \) and \( M \), respectively, and the mod function is the remainder function. In the above process, the probability of calculating the key \( y \) only if the values of \( i \) and \( e \) are known is 0, so under the RSA algorithm, only the data owner has the key, which ensures the security of data transmission.

3.5. Computer Communication Encryption and Decryption Combining 3DES Algorithm and RSA Algorithm. Figures 3 and 4, respectively, show the process of encrypting and decrypting data communication by combining the RSA algorithm with the 3DES algorithm, the function of the RSA algorithm is to encrypt the key of the 3DES algorithm to provide double guarantees for data security transmission.

The analysis of the encryption process of computer communication data is as follows:

First, in the data encryption operation, the 3DES key is obtained based on the arbitrary number and operation function, that is, the 168-bit key \( K \); Then the plaintext of the computer data to be transmitted is encrypted, the tools used are the key \( K \) and the algorithm 3DES, the result is ciphertext, and the generated public key is stored in the server by \( i \) and \( e \); Based on the RSA algorithm, the 168-bit key \( K \) of 3DES is encrypted, the encrypted key is set to \( XK \), and \( XK \) is fused with the ciphertext, which is the final ciphertext for transmission [18].

The analysis of the computer communication data decryption process is as follows: After the receiving end obtains the encrypted data, it reads the public key in the
server, first decrypts the key k of the 3DES algorithm based on the public key and the private key, then decrypts the communication ciphertext based on the key k, and finally reads the data transmitted by the sending end securely.

4. Analysis of Results

A data transmission encryption and decryption simulation test platform is built in a local area network communication environment, the sender’s computer is named A, and the receiver’s computer is named B. 5 groups of data of the same size are selected for communication, and 50 brute force attacks are artificially set to crack the data transmission security key. In order to verify the security performance of the author’s method to encrypt communication data, 3DES encryption algorithm, DES encryption algorithm and article algorithm are used, at the same time, data encryption simulation experiments are carried out, the analysis results of the security performance and encryption and decryption efficiency of each algorithm are as follows. Under 50 brute-force attacks, after the data communication encrypted by the three algorithms, the average damage degree of each transmission is shown in Figure 5.

Among them, the author’s algorithm has the least damage to data communication after encryption, only the second and third groups of data were damaged by 0.012% and 0.011%, the third and fourth groups of data encrypted by the 3DES encryption algorithm had weak security performance, and 0.11% and 0.10% of the data were damaged. In contrast, the encryption performance of the DES encryption algorithm is not ideal, and about 0.10 to 0.32% of the data is damaged in the transmission of data through the local area network. It can be seen that the data security performance encrypted by the author’s algorithm is the best. The 3DES encryption algorithm is to solve the problem of insufficient security of the original DES encryption algorithm. Since a large number of practical application cases have proved that the security performance of the DES encryption algorithm does not meet the requirements of modern data transmission, the key length of the DES algorithm is increased to 168 bits, the author uses the encryption algorithm after the key extension, which improves the encryption performance [19]. Compared with the 3DES encryption algorithm, the author uses RSA to encrypt the 3DES key, which further improves the effectiveness of data encryption.

As can be seen from Figure 6, the DES encryption algorithm takes the shortest time, and the 3DES encryption algorithm takes the longest time, this is because the 3DES encryption algorithm increases the key length on the basis of the original algorithm, so the operation time is prolonged. Although the author’s algorithm is not as efficient as the DES algorithm, the difference is only about 1 ms, and the optimal encryption effect is guaranteed at the same time. Therefore, in general, among the three algorithms, the article algorithm has the best security performance in computer communication.

5. Conclusion

The author combines the strong security of the 3DES encryption algorithm and the asymmetric encryption advantages of the RSA algorithm, a new computer communication data encryption strategy is formed. After experimental verification, the encryption algorithm proposed by the author has achieved good results in terms of security performance and response efficiency, it is suitable for actual computer data communication scenarios and can effectively improve computer security management.
Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Funding

This study did not receive any funding in any form.

References


